A GUIDE TO SERRE'S *A COURSE IN ARITHMETIC*

COLIN NI

Abstract. This paper exposits Serre's book [1] on number theory. It presents motivating examples, heuristic arguments to justify ideas, and a summary of results for each chapter. We hope to aid future readers of this classic.

Contents

Number theoretic questions often lead to powerful mathematics. For example, to prove Legendre's conjecture that every arithmetic progression $a, a+d, a+2d, \ldots$ for coprime a and d contains an infinite number of primes, Dirichlet invented his L functions in 1837, and since then L functions and their generalizations have become a focus in modern mathematics. The Birch and Swinnerton-Dyer conjecture, one of the seven millennium prize problems, revolves around L functions for elliptic curves. Moreover, the reciprocity conjecture of the Langlands program, perhaps the biggest project in modern mathematics, studies automorphic L functions attached to certain representations of the general linear group.

Number theory gives rise to and helps explain strange phenomena; for instance, the following incredible yet related facts are scattered throughout Serre's book. In 8 dimensions, at most 240 spheres can touch a common sphere without overlap. This *kissing number* is realized by an arrangement via the Γ_8 lattice, the only unimodular lattice of rank 8. More generally, the study of spaces of modular forms determines that the Γ_8 lattice has $240\sigma_3(m)$ vectors of squared norm $2m$, where $\sigma_k(m)$ is the sum of the kth powers of the divisors of m, and it is the root system of E_8, one of the five exceptional cases in the Cartan-Killing classification of complex simple Lie algebras. Analogously in 24 dimensions, the bound is 196560 spheres and is realized by the Leech lattice, the only one of the 24 unimodular lattices with rank 24 without a vector of squared norm 2. The Leech lattice has exactly $\frac{65520}{691}(\sigma_{11}(m) - \tau(m))$ vectors of squared norm $2m$, where τ is the Ramanujan function. The quotient of its automorphism group by its center is Co_1, one of the 26 sporadic cases in the classification of finite simple groups.

We aim to highlight these motivations and phenomena in this paper.

1. Finite fields

Quadratic reciprocity provides a way to compute whether or not a number is a square mod p. The *Legendre symbol* records this information as

$$\left(\frac{\ell}{p}\right) = \begin{cases} +1 & \text{if } \ell \text{ is a square mod } p \\ -1 & \text{otherwise,} \end{cases}$$

for instance $\left(\frac{37}{47}\right) = 1$ since $37 \equiv 15^2 \bmod 47$ but $\left(\frac{38}{47}\right) = -1$ since 38 is not, which the following Python command confirms:

```
>>> 38 in [(n ** 2) % 47 for n in range(47)]
False
```

For odd distinct primes p, q the *quadratic reciprocity* law [Thm I.6] reads

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}.$$

After observing the Legendre symbol is multiplicative and proving

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = \pm 1 \bmod 8 \\ -1 & \text{otherwise} \end{cases}$$

[Thm I.5(*iii*)], computing Legendre symbols becomes a simple matter of flipping and factoring, for instance

$$\left(\frac{37}{47}\right) = \left(\frac{47}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -1 \cdot \left(\frac{37}{5}\right) = -1 \cdot \left(\frac{2}{5}\right) = +1$$

versus

$$\left(\frac{38}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{19}{47}\right) = 1 \cdot \left(\frac{19}{47}\right) = -\left(\frac{47}{19}\right) = -\left(\frac{9}{19}\right) = -1,$$

which agrees with our initial observations.

The quadratic reciprocity law is of fundamental importance. It was first proved by Gauss in 1801 in his book *Disquisitiones Arithmeticae* and since then more than 240 proofs have been published. According to Wikipedia, it has motivated enormous branches of mathematics:

> Since Gauss, generalizing the reciprocity law has been a leading problem in mathematics and has been crucial to the development of much of the machinery of modern algebra, number theory, and algebraic geometry, culminating in Artin reciprocity, class field theory, and the Langlands program.

One such proof of quadratic reciprocity, purely algebraic, is given in Serre and relies on the following elementary properties of finite fields. Finite fields have prime power $q = p^f$ order, and conversely there is exactly one field $\mathbb{F}_q$ up to isomorphism for each such prime power [Thm I.1]; the construction uses Galois theory, taking the fixed subfield of the fth iterate of the Frobenius automorphism $x \mapsto x^p$ on an algebraically closed field of characteristic p. Moreover, the multiplicative groups of finite fields are cyclic [Thm I.2], in symbols $\mathbb{F}_q^* \cong \langle x \mid x^{q-1} = 1 \rangle$. This implies that when $p \neq 2$ the index of $\mathbb{F}_q^{*2}$ is two [Thm I.4] since it fits in the exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{F}_q^{*2} & \longrightarrow & \mathbb{F}_q^* & \longrightarrow & \{\pm 1\} & \longrightarrow & 1 \\ & & & & x & \longmapsto & x^{\frac{q-1}{2}}. & & \end{array}$$

The key observation of finite fields used in the proof of reciprocity drops out of these facts, namely that there is the same number of squares as nonsquares in any finite field. Specifically, this key observation furnishes the identity

$$\sum_{\ell \in \mathbb{F}_p} \left(\frac{\ell}{p}\right) = 0$$

used in Lemma 1 to Thm I.6. Additionally, a cute application of this key observation shows that every element in a finite field can be written as a sum of two squares. To see this, note the squares in $\mathbb{F}_q$ are precisely $\mathbb{F}_q^{*2} \cup \{0\}$ which has cardinality $\frac{q+1}{2}$, but in general if $A, B \subset G$ are subsets of an additively written group such that $|A| + |B| > |G|$, then $A + B = G$.

The Chevalley-Warning theorem [Thm I.3] also depends on these facts. It states that for a family of polynomials

$$f_\alpha \in \mathbb{F}_q[X_1, \dots, X_n] \quad \text{satisfying} \quad \sum_\alpha \deg f_\alpha < n,$$

the number of common zeros in $\mathbb{F}_q^n$ a multiple of p. As a specific corollary, any homogeneous degree two polynomial in at least three variables over $\mathbb{F}_q$ has a nontrivial zero. The fact that $\mathbb{F}_q^*$ is cyclic goes into proving for a number $u \geq 0$ the identity

$$\sum_{x \in \mathbb{F}_q} x^u \equiv \begin{cases} -1 & \text{if } u \geq 1 \text{ and } q-1 \text{ divides } u \\ 0 & \text{otherwise.} \end{cases}$$

More importantly, there is a take-away idea in the proof of the Chevelley theorem, namely to construct a characteristic function χ_V for the set V of common zeros via

$$\chi_V = \prod_\alpha (1 - f_\alpha^{q-1}) = \begin{cases} 1 & \text{on common zeros} \\ 0 & \text{elsewhere} \end{cases}$$

and then rewriting the desired result as

$$|V| = \sum_{x \in \mathbb{F}_q^n} \chi_V(x) \equiv 0 \bmod p.$$

Now it is quick to complete the proof. Note χ_V is a linear combination of monomials; by hypothesis they all have degree $< n(q-1)$, so for any monomial $X^u = X_1^{u_1} \dots X_n^{u_n}$ we have by the pigeonhole principle $u_k < q-1$ for some k. Hence by the identity it follows that

$$\sum_{x \in \mathbb{F}_q^n} x^u = \sum_{x \in \mathbb{F}_q^{n-1}} x_1^{u_1} \dots \widehat{x_k^{u_k}} \dots x_n^{u_n} \sum_{x \in \mathbb{F}_q} x_k^{u_k} \equiv 0,$$

where the hat denotes omission.

2. p-ADIC FIELDS

The p-adic field $\mathbb{Q}_p$ enlarges the field of rational numbers $\mathbb{Q}$. A heuristic view on p-adic numbers is that they are base p numbers that trail off to the left, where two numbers are considered closer the more numbers on which they agree starting from the right. This admits a well-defined addition and multiplication of infinite numbers in the usual way from elementary school. For example, in the 7-adics

$$\overline{21}.5 = \dots 12121.5 \in \mathbb{Q}_7 \quad \text{and} \quad \dots 666.34 = 44$$

since the sequence $1, 10, 100, \ldots$ approaches both 0 and the difference $44-\ldots 666.34$. Furthermore, any rational number can be written this way, for instance $\frac{1}{5} = \overline{12102}$ in $\mathbb{Q}_3$ since $\overline{0121} + \overline{12102} = \overline{2} = 0$ and

$$-\frac{1}{5} = \frac{16}{1-3^4} = \left(3^2 + 2\cdot 3^1 + 3^0\right)\sum_{i=0}^{\infty} 3^{4i} = \overline{0121},$$

noting that the infinite sum converges in the 3-adics.

There are two popular constructions of the p-adics, one algebraic and one analytic, each of which highlights different topological properties.

For the analytic construction, on $\mathbb{Q}$ define the *p-adic valuation*

$$v_p(x) = \text{the unique } n \in \mathbb{Z} \text{ such that } x = p^n \cdot \frac{a}{b} \text{ where } p \nmid a, b$$

and then the *p-adic metric*

$$d(x,y) = \frac{1}{e^{v_p(x-y)}}$$

which realizes this intuition of closeness, then take the completion of $\mathbb{Q}$ with respect to the metric. This analytic construction of $\mathbb{Q}_p$ makes $\mathbb{Q}$ dense by definition, and restricting this construction to $\mathbb{Z}$ constructs the p-adic integers $\mathbb{Z}_p$

On the other hand, there is the following algebraic construction. Let $\mathbb{Z}_p$ be the categorical (inverse) limit of the sequence

$$\cdots \longrightarrow \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{\phi_3} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\phi_2} \mathbb{Z}/p\mathbb{Z}$$

of rings with canonical maps, or equivalently let

$$\mathbb{Z}_p = \left\{ (\ldots, x_3, x_2, x_1) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; \phi(x_n) = x_{n-1} \text{ for all } n \geq 2 \right\}$$

be a ring with coordinate-wise addition and multiplication. Endow each $\mathbb{Z}/p^n\mathbb{Z}$ with the discrete topology and $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ with the product topology. This construction of $\mathbb{Z}_p$ makes it clear that it is compact: the product space is compact by Tychonoff's theorem, and $\mathbb{Z}_p$ is closed in it because if $(x_n) \notin \mathbb{Z}_p$, then $\phi(x_k) \neq x_{k-1}$ for some $k \geq 2$, whence

$$\prod_{n=k+1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \times \{x_k\} \times \{x_{k-1}\} \times \prod_{n=1}^{k-2} \mathbb{Z}/p^n\mathbb{Z}$$

is an open set containing (x_n).

Now the following brief algebraic examination of the group of units $\mathbb{U}$ in $\mathbb{Z}_p$ leads to a metrization of this topology and also to the algebraic construction of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ can be written uniquely in the form $p^n u$ with $u \in \mathbb{U}$ and $n \in \mathbb{Z} \cup \{\infty\}$ where we set where $p^\infty = 0$ [Prop II.2], so defining $v_p(x)$ to be this number n metrizes $\mathbb{Z}_p$ via the same distance function as before. Furthermore, the identities

$$v_p(xy) = v_p(x) + v_p(y) \quad \text{and} \quad v_p(x+y) \geq \min(v_p(x), v_p(y))$$

show that $\mathbb{Z}_p$ is an integral domain. Using this to define $\mathbb{Q}_p$ as the field of fractions of $\mathbb{Z}_p$, the algebraic description of $\mathbb{U}$ accounts for the identity $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$, so the metric on $\mathbb{Z}_p$ extends to $\mathbb{Q}_p$ via the same distance function.

Working in the p-adics has its merits and downsides. The main downside is that having a solution in $\mathbb{Q}_p$ of an equation does not guarantee a solution in $\mathbb{Q}$. For

instance, we will see momentarily that $f(x) = x^2 - 2$ has a root in $\mathbb{Q}_7$, but certainly $\sqrt{2} \notin \mathbb{Q}$. On the other hand, algebraically $\mathbb{Q}_p$ is well understood. In fact we have seen that $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{U}$, and an involved analysis of the group of units $\mathbb{U}$ via the subgroups $\mathbb{U}_n = 1 + p^n\mathbb{Z}_p$ produces the description

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{for } p \neq 2$$

[Thm II.2]. Furthermore, the convergence properties of the p-adics make it particularly nice on which to do analysis and find solutions to equations, largely due to the following result.

Hensel's lifting lemma lifts roots of polynomials mod p^n to the p-adics. It does this by successively lifting roots to still be roots mod higher powers of p while also converging to a root in $\mathbb{Z}_p$. To illustrate, for $f(x) = x^2 - 2$ we may successively lift the root $f(4) = 14 \equiv 0 \bmod 7$ to

$$\begin{aligned}
&f(4 + 5 \cdot 7^1) = 1519 \equiv 0 \bmod 7^2 \\
&f(4 + 5 \cdot 7^1 + 4 \cdot 7^2) = 55223 \equiv 0 \bmod 7^3 \\
&f(4 + 5 \cdot 7^1 + 4 \cdot 7^2 + 0 \cdot 7^3) = 55223 \equiv 0 \bmod 7^4 \\
&f(4 + 5 \cdot 7^1 + 4 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4) = 149817598 \equiv 0 \bmod 7^5,
\end{aligned}$$

and we observe that the roots are beginning to converge in the 7-adics because we are adjusting the roots by higher and higher powers of 7. This is analogous to Newton's method which uses the intersection of a tangent line with the x-axis to iteratively approach a root of a differentiable function, taking smaller and smaller steps. Motivated by this, a baby version of Hensel's lemma states that if

$$f(a) \equiv 0 \bmod p \quad \text{and} \quad f'(a) \not\equiv 0 \bmod p \quad \text{for} \quad a \in \mathbb{Z}_p \text{ and } f \in \mathbb{Z}_p[X],$$

then there exists a p-adic zero $\alpha \in \mathbb{Z}_p$ of f such that $a \equiv \alpha \bmod p$. For instance $f \in \mathbb{Z}_7[X]$ above has a 7-adic root since $f'(4) = 6 \not\equiv 0 \bmod p$. The full statement [Thm II.1] is more general, taking into account an approximal root mod p^n and guaranteeing a closer final root depending on the valuation of the derivative.

3. Hilbert symbol

The *Hilbert symbol* is related to the Legendre symbol; it has a reciprocity law which generalizes quadratic reciprocity, but it is a global property of the symbol as opposed to a local property. Hilbert introduced the symbol in 1897, though only for global fields, and the symbol has since been realized in terms of the Artin symbol from local class field theory. The setting for the symbol is over a field k, which is taken to be either the p-adic numbers $\mathbb{Q}_p$ or the real numbers $\mathbb{R}$.

The Hilbert symbol is defined for $a, b \in k^*$ as

$$(a,b) = \begin{cases} +1 & \text{if } z^2 = ax^2 + by^2 \text{ has a zero solution in } k^3 \\ -1 & \text{otherwise.} \end{cases}$$

Certainly this defines a map $k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}$ because the symbol is invariant up to multiplication of a, b by squares, but moreover straightforward deductions establish that it is a nondegenerate bilinear form on the $\mathbb{F}_2$-vector space k^*/k^{*2} [Thm III.2]. This follows from the following formulas for Hilbert symbols.

There is a clean identity for the Hilbert symbol in terms of the Legendre symbols, namely by writing $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{U}$, we have

$$(a,b) = \begin{cases} (-1)^{\alpha\beta\cdot\frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}+\alpha\cdot\frac{v^2-1}{2}+\beta\cdot\frac{u^2-1}{2}} & \text{if } p = 2 \end{cases}$$

[Thm III.1], where we identity $u, v \in \mathbb{U}$ via their canonical images in $\mathbb{U}/\mathbb{U}_1 \cong \mathbb{F}_p^*$. Checking this identity amounts to case work for the parity of α, β, and funnily enough $\alpha = \beta = 0$ is the nontrivial case. Here to show $(u, v) = 1$, one argues that $z^2 = ux^2 + vy^2$ reduced mod p has a nontrivial solution by the mentioned corollary to the Chevellay theorem, hence since its discriminant is a p-adic unit, the solution lifts by a corollary to Hensel's lemma. Moreover certainly for the case of the nonzero real numbers we have

$$(a,b) = \begin{cases} +1 & \text{if } a \text{ or } b > 0 \\ -1 & \text{if } a \text{ and } b < 0 \end{cases} \qquad \text{for } a, b \in \mathbb{R}^*.$$

The Hilbert reciprocity law [Thm III.3] is as follows. Set $V = \{\text{primes}\} \cup \{\infty\}$, set $\mathbb{Q}_\infty = \mathbb{R}$, and for $a, b \in \mathbb{Q}^*$ denote by $(a, b)_p$ the Hilbert symbol of their images in $\mathbb{Q}_p$. The global product formula reads

$$\prod_{v \in V} (a,b)_v = 1 \quad \text{where } (a,b)_v = 1 \text{ for almost all } v \in V.$$

This generalizes quadratic reciprocity when a, b are distinct odd primes since

$$(a,b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}, \quad (a,b)_a = \left(\frac{b}{a}\right), \quad (a,b)_b = \left(\frac{a}{b}\right), \quad \text{and} \quad (a,b)_\infty = 1$$

by the above identities and $(a, b)_v = 1$ for the other cases.

4. Quadratic forms over $\mathbb{Q}_p$ and over $\mathbb{Q}$

Number theory is among many fields that study quadratic forms. According to Wikipedia:

> Quadratic forms occupy a central place in various branches of mathematics, including number theory, linear algebra, group theory (orthogonal group), differential geometry (Riemannian metric, second fundamental form), differential topology (intersection forms of four-manifolds), and Lie theory (the Killing form).

At the most elementary viewpoint, number theory is frequently concerned with the values that a quadratic form nontrivially takes, in other words the values it *represents*. As one example, Lagrange's four square theorem states that the quadratic form $f(w, x, y, z) = w^2 + x^2 + y^2 + z^2$ represents all positive numbers. More generally, if any positive definite quadratic form with integer matrix represents the 15 numbers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \text{ and } 15,$$

then it represents all positive integers. Incredibly enough, for an integral quadratic form, it suffices for the form to represent the 29 numbers

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23,$$
$$26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, \text{ and } 290,$$

and furthermore this is sharp in the sense that for any one number omitted there exists a form representing the other 28 numbers but not the omitted one. These results were proved respectively in 1993 by John Conway and William Schneeberger and in 2008 by Manjul Bhargava and Jonathan Hanke.

Quadratic forms are degree two homogeneous polynomials that can be written

$$f(X_1, \dots, X_n) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j$$

with coefficients in a field k whose characteristic we assume to be distinct from 2. Viewing two forms f and f' as bilinear forms on k^n, they are equivalent and written $f \sim f'$ if there exists a coordinate change between them. For instance $X_1 X_2 \sim X_1^2 - X_2^2$ via the coordinate change

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \text{or in other words} \quad \begin{matrix} X_1 \mapsto X_1 - X_2 \\ X_2 \mapsto X_1 + X_2, \end{matrix}$$

and forms of this type are called *hyperbolic* because their nonzero level sets are hyperbolas in $\mathbb{R}^2$. More precisely $f \sim f'$ if there exists $\Phi \in \mathrm{GL}_n(k)$ such that $f = f' \circ \Phi$ or, alternatively, if their matrices are equivalent in the sense that $A = XA'X^T$ for some $X \in \mathrm{GL}_n(k)$.

Naturally, quadratic forms act on k^n as symmetric bilinear forms, so the strategy is to study all *quadratic modules*, finite dimensional vector spaces over k equipped with such forms, and then relay the results back. Quadratic modules are more general than inner product spaces because there is no requirement of positive-definiteness; thus there are *isotropic* vectors, that is, nonzero norm zero vectors. Carrying on the example, the module associated to a hyperbolic quadratic form is generated by two nonorthogonal isotropic vectors, namely $(1, 0)$ and $(0, 1)$ which have norm zero because they are on the height zero level set but which are nonorthogonal because their sum lies on the height one level set. Catering to the strategy, note $f \sim f'$ just says their corresponding modules are isomorphic, and for two forms $f(X_1, \dots, X_n)$ and $g(X_1, \dots, X_m)$ we write $f \dot{+} g$ for the form

$$f(X_1, \dots, X_n) + g(X_{n+1}, \dots, X_{n+m}),$$

which corresponds to a direct sum of quadratic modules.

We now state and harvest the core results from studying quadratic modules. Every quadratic module has an orthogonal basis [Thm IV.1], so every quadratic form f in n variables is equivalent to $a_1 X_1^2 \dot{+} \dots \dot{+} a_n X_n^2$ for some $a_1, \dots, a_n \in k$. Isomorphic subspaces of such modules have isomorphic orthogonal complements [Cor to Thm IV.3], and this translates to Witt's cancellation theorem, which asserts that if $g \dot{+} h \sim g' \dot{+} h'$ and $g \sim g'$, then $h \sim h'$. Since every isotropic vector is contained in a hyperbolic plane [Prop IV.3], degenerate forms decompose into $g_1 \dot{+} \dots \dot{+} g_m \dot{+} h$ where $g_1, \dots, g_m$ are hyperbolic and h does not represent zero, and this is unique by cancellation.

These results provide the language for the classification of forms over $\mathbb{Q}_v$, which involve the following invariants. If $f \sim a_1 X_1^2 \dot{+} \dots \dot{+} a_n X_n^2$, then the number of the a_i that are nonzero is called its *rank* r, the product of them its *discriminant* d, and the form f *nondegenerate* if it has rank n. If f is p-adic, then the Hilbert symbol is defined, so we set

$$\epsilon(f) = \prod_{i<j} (a_i, a_j).$$

This number is invariant of the chosen associated module [Thm IV.5], which follows from a result in quadratic modules asserting that there is a finite chain of orthogonal bases contiguously relating any two orthogonal bases [Thm IV.2]. Finally when f is real its *signature* tracks the number of a_i that are negative, zero, and positive.

The classification of quadratic forms over all of our familiar fields is as follows:

$$\begin{aligned} \text{finite fields } \mathbb{F}_q &- \text{ rank and discriminant} \\ p\text{-adics } \mathbb{Q}_p &- \text{ rank, discriminant, and } \epsilon \\ \text{real numbers } \mathbb{R} &- \text{ signature} \\ \text{rationals } \mathbb{Q} &- \text{ over all } \mathbb{Q}_v. \end{aligned}$$

The proof of this classification requires much work. The main technical work goes into the classification over $\mathbb{Q}_p$, in particular that a rank n quadratic form f represents $a \in k^*/k^{*2}$ if and only if

$$\begin{aligned} & n = 1 \text{ and } a = d \\ \text{or } & n = 2 \text{ and } (a, -d) = \epsilon \\ \text{or } & n = 3 \text{ and } a \neq d \text{ or else } (-1, -d) = \epsilon \\ \text{or } & n \geq 4 \end{aligned}$$

[Cor to Thm IV.6], which in particular shows that equivalent forms represent the same values. Thus if f and g have the same invariants, then we have $f \sim aZ^2 \dot{+} f'$ and $g \sim aZ^2 \dot{+} g'$ for some $a \in k^*/k^{*2}$ and rank $n-1$ forms f' and g' [Cor 1 to Prop IV.3'], so since squares vanish

$$d(f') = ad(f) = ad(g) = d(g'),$$

hence

$$\epsilon(f') = \epsilon(f)(a, d(f')) = \epsilon(g)(a, d(g')) = \epsilon(g').$$

Now by induction on rank it follows that $f \sim g$.

The Hasse-Minkowski theorem classifies quadratic forms over $\mathbb{Q}$ and resolves the issue displayed in §3 that a local solution in $\mathbb{Q}_p$ does not guarantee a solution in $\mathbb{Q}$. For concrete intuition and motivation, consider the equation $x^3 - 2x + 17 = 0$. It does not have an integer solution because it does not have one mod 5, which one checks easily; in other words, it does not have a global solution because it does not have a local solution at some place. Conversely, this raises the question of whether a local root everywhere should piece together a global root. The Hasse-Minkowski theorem answers in the affirmative for quadratic forms (viewing $\mathbb{R}$ as a local place), and for this reason it is called the local global principle. In particular, it asserts that if an integral quadratic form represents a number over $\mathbb{R}$ and mod p for every p, then it represents the number over $\mathbb{R}$.

Precisely, the *Hasse-Minkowski theorem* [Thm IV.8] states that a quadratic form f represents 0 over $\mathbb{Q}$ if and only if it does over all $\mathbb{Q}_v$, and by a similar induction on rank and applying Witt's cancellation theorem, it follows that two forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent over all $\mathbb{Q}_v$ [Thm IV.9]. The proof of Hasse-Minkowski is a celebration of the objects and techniques developed in the first part of the book; it uses many major results nontrivially and involves every core idea. Serre states in the preface that the goal of the first four chapters is to achieve this theorem.

The theorem is extremely deep and powerful, so typically today Hasse-Minkowski

is proved via class field theory which is even more so. Serre's comparatively elementary proof in fact depends on Dirichlet's theorem on arithmetic progressions, which is proved later in the sixth chapter of the book. Nothing from the sixth chapter uses anything from the first five, so there is no circular logic.

Unfortunately Hasse-Minkowski does not extend to cubic forms, degree 3 homogenous polynomials; the key counterexample is the one by Ernst Selmer:

$$3x^3 + 4y^3 + 5z^3 = 0.$$

Indeed with some effort one demonstrates it has a solution over $\mathbb{R}$ and all $\mathbb{Q}_p$. However, it does not have a solution over $\mathbb{Q}$, which requires some difficult algebraic number theory and the theory of elliptic curves to prove.

A serious application is Lagrange's four square theorem. Gauss's theorem is the intermediate step, implying the four square theorem immediately; it states that n being a sum of three squares is equivalent to the condition that n not be of the form $4^a(8b-1)$. A study of the 2-adics [Thm II.4] reveals that this condition just says $-n$ is a square in $\mathbb{Q}_2^*$, but Hasse-Minkowski shows that $f = x^2 + y^2 + z^2$ represents $a \in \mathbb{Q}^*$ if and only if $a > 0$ and $-a$ is not a square in $\mathbb{Q}_2^*$ since $n = 3$ and $(-1, -d) = \epsilon$. Finally an elementary but intricate argument [Lemma B in the appendix of IV] shows that for a quadratic forms of this kind a rational solution implies the existence of an integer solution.

5. Integral quadratic forms with discriminant ± 1

Also known as unimodular lattices, these quadratic forms and their associated modules arise in many areas, for example in string theory, sphere packings, and low dimensional topology. For the latter, according to Wikipedia:

> The second cohomology group of a closed simply connected oriented topological 4-manifold is a unimodular lattice. Michael Freedman showed that this lattice almost determines the manifold: there is a unique such manifold for each even unimodular lattice, and exactly two for each odd unimodular lattice. In particular if we take the lattice to be 0, this implies the Poincaré conjecture for 4-dimensional topological manifolds. Donaldson's theorem states that if the manifold is smooth and the lattice is positive definite, then it must be a sum of copies of $\mathbb{Z}$, so most of these manifolds have no smooth structure. One such example is the E_8 manifold [the compact simply connected 4-manifold with intersection form the E_8 lattice].

The condition for an integral quadratic form to have discriminant ± 1 is equivalent to its associated quadratic module to be isomorphic to its dual, viewing it in the category of free abelian groups of rank n equipped with symmetric bilinear forms and metric-preserving homomorphisms. Let S_n be the full subcategory of such objects, and let $S = \bigcup_n S_n$. Compared to the category of quadratic modules over $\mathbb{Z}$, the equivalence classes of objects here are finer since the change of coordinate matrices must be integral.

Let S_n be the full subcategory of such objects, and let $S = \bigcup_n S_n$. Compared to the category of quadratic modules over $\mathbb{Z}$, the equivalence classes of objects here are finer since the change of coordinate matrices must be integral.

There are two crucial examples of such lattices. The first is $I_+, I_- \in S_1$, both $\mathbb{Z}$ but with respective quadratic forms $+xy$ and $-xy$. The second is $\Gamma_{8m} \in S_{8m}$

for $m > 0$ constructed as follows. In $\mathbb{Z}^{8m}$ viewed in $\mathbb{Q}^{8m}$ and with the induced usual bilinear form $\Sigma x_i y_i$, take the submodule E generated by $e = \left(\frac{1}{2}, \ldots, \frac{1}{2}\right)$ and by elements with even square norm. One checks the discriminant is $+1$ and that $x = (x_1, \ldots, x_{8m}) \in E$ if and only if

$$2x_i \in \mathbb{Z}, \quad x_i - x_j \in \mathbb{Z}, \quad \text{and } \Sigma x_i \in 2\mathbb{Z},$$

hence $x.e = \frac{1}{2}\Sigma x_i$ and $e.e = 2k$ and so $x.x$ is even. Thus Γ_{8m} is even and in S_{8m}.

The case Γ_8 is particularly special since it arises as the root system for E_8, one of the five exceptional cases in the Cartan-Killing classification of complex simple Lie algebras and which has corresponding Dynkin diagram

A *root system of rank* r is a collection of vectors, called roots, which span an r-dimensional Euclidean space and are invariant under reflection through the hyperplane perpendicular to any root. In Γ_8 resides a root system of rank r consisting of the

$$240 = 4 \cdot \binom{8}{2} + \sum_{i=0}^{4} \binom{8}{2i}$$

elements with square norm two in Γ_8, namely the permutations of the entires of $(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0)$ and the vectors $\left(\pm\frac{1}{2}, \ldots, \pm\frac{1}{2}\right)$ which have an even number of $+\frac{1}{2}$ entries. They generate Γ_8, for instance via the basis

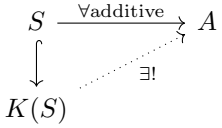
$$\left(+\frac{1}{2}, -\frac{1}{2}, \ldots, -\frac{1}{2}, +\frac{1}{2}\right), \quad e_1 + e_2, \quad \text{and} \quad e_i - e_{i-1} \text{ for } 2 \leq i \leq 7.$$

For $m \geq 1$, however, the vectors of square norm two do not generate Γ_{8m}, so in particular $\Gamma_8 \oplus \Gamma_8 \ncong \Gamma_{16}$.

Consider the following invariants attached to any lattice $E \in S$:

- rank n determined by $E \in S_n$
- index $\tau = r - s$, where (r, s) is the signature obtained from extending scalars to the real numbers by tensoring with $\mathbb{R}$
- discriminant d from before, which here is equal to $(-1)^{\frac{s}{2}}$
- even, otherwise odd, if the quadratic form takes only even values
- ϵ_p, obtained by tensoring with $\mathbb{Q}_p$

Indefinite lattices of S are classified by rank, index, and type [Thm V.6]. More generally, the Grothedieck group $K(S)$ of the category S with respect to $\oplus$ is free abelian, generated by I_+ and I_- [Thm V.1], where we recall that the Grothendieck construction $K(S)$ on a commutative monoid S formally inverts elements in the most efficient way or, in other words, to satisfy the following universal property:



Proving this requires an application of Hasse-Minkowski, in particular to show that if $E \in S$ is indefinite, then the quadratic module $E \otimes \mathbb{Q}$ hence also E represents zero [Thm V.3]; to do this one checks that $E \otimes \mathbb{Q}$ represents zero over all $\mathbb{Q}_v$.

There are a finite number of definite lattices of S for each rank; this follows from

the reduction theory of quadratic forms, omitted from the book. To determine explicitly the set C_n of isomorphism classes of even rank $n = 8k$ lattices, one uses the Minkowski-Siegel formula

$$\sum_{E \in C_n} \frac{1}{g_E} = \frac{B_{2k}}{8k} \prod_{j=1}^{4k-1} \frac{B_j}{4j},$$

where B_i is the ith Bernoulli number and where g_E is the order of the automorphism group of E, which is finite because it is a discrete subgroup of the orthogonal group. For Γ_8 we have $g_{\Gamma_8} = 696729600 = 2^{14}3^5 5^2 7$, so since

$$\frac{B_2}{8} \prod_{j=1}^{3} \frac{B_j}{4j} = \frac{\frac{1}{30}}{8} \cdot \frac{\frac{1}{6}}{4} \cdot \frac{\frac{1}{30}}{8} \cdot \frac{\frac{1}{42}}{12} = \frac{1}{696729600},$$

it must be that Γ_8 is the unique lattice of C_8. Similarly in C_{16} there are certainly two lattices Γ_{16} and $\Gamma_8 \oplus \Gamma_8$ which have respectively $g_{\Gamma_{16}} = 2^{15} \cdot 16!$ and $g_{\Gamma_8 \oplus \Gamma_8} = 2g_{\Gamma_8}^2 = 2^{29}3^{10}5^4 7^2$, so since

$$\frac{B_4}{16} \prod_{j=1}^{7} \frac{B_j}{4j} = \frac{\frac{1}{30}}{16} \cdot \frac{\frac{1}{6}}{4} \cdot \frac{\frac{1}{30}}{8} \cdot \frac{\frac{1}{42}}{12} \cdot \frac{\frac{1}{30}}{16} \cdot \frac{\frac{5}{66}}{20} \cdot \frac{\frac{691}{2730}}{24} \cdot \frac{\frac{7}{6}}{28} = \frac{1}{2^{15} \cdot 16!} + \frac{1}{2^{29}3^{10}5^4 7^2},$$

it must be that C_{16} is comprised of precisely these two lattices. Hans-Volker Niemeier classified the lattices in C_{24} in 1968 and found 24 elements, every one of which except for the *Leech lattice* Λ contains an element with square norm 2. The Leech lattice has automorphism group Co_0 of order

$$g_\Lambda = 2^{22}3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23 = 8315553613086720000,$$

and the quotient of this group by its center $\{\pm 1\}$ is Co_1, one of the 26 sporadic finite simple groups.

6. The theorem on arithmetic progressions

Dirichlet's prime number theorem states that for any two positive coprime integers a and d, the arithmetic sequence

$$a, \quad a+d, \quad a+2d, \quad a+3d, \ldots$$

contains infinitely many prime numbers. Ben Green and Terence Tao in 2004 proved a sort of converse that there exist arbitrarily long arithmetic sequences of primes;

$$43142746595714191 + 23681770 \cdot 223092870 \cdot n \qquad \text{for } n = 0, \ldots, 25$$

is one of the longest such sequences known.

The core idea in proving Dirichlet's theorem is to rephrase it in terms of density. Setting $P = \{\text{primes}\}$, define the Riemann zeta function by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}.$$

The identity between the sum and product is the Euler product formula and is given by sieving the primes in the series as in Eratosthenes. Without analytic

continuation it is holomorphic on $R(s) > 1$ and has a simple pole at $s = 1$, and its log may be written in the form

$$\log \zeta(s) = \sum_{p \in P} \log\left(1 - \frac{1}{p^s}\right) = -\sum_{p \in P} \sum_{s=1}^{\infty} \frac{1}{kp^{ks}}, \quad \text{where } \sum_{p \in P} \sum_{s \geq 2} \frac{1}{kp^{ks}} \text{ is bounded}$$

[Prop VI.10 and its Cor 2]. Thus the *density of a subset* $A \subset P$ may be defined as

$$\lim_{s \to 1} \left(\sum_{p \in A} \frac{1}{p^s} \right) \Big/ \log \frac{1}{s-1} \quad \text{using that} \quad \sum_{p \in P} \frac{1}{p^s} \sim \log \frac{1}{s-1} \quad \text{as } s \to 1.$$

Now a stronger version of the theorem asserts $P_a = \{\text{primes coprime to } a\}$ has density $1/\phi(m)$, where obviously if P_a were finite, then it would have density zero. Intuitively, this stronger statement says the primes are fairly distributed mod m, so for instance there are as many primes ending in 1 as there are 3, 7, and 9.

Before introducing the Dirichlet L series, which are the main technical objects in the proof of Dirichlet's theorem, we discuss more generally *Dirichlet series* which are of the form

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}.$$

Dirichlet series generalize series of the form a_n/n^s as well as power series. They converge on open half planes [Cor 2 to Prop VI.6] and often on planes of the form $\operatorname{Re} z > \rho$, in which case we call ρ the *abscissa of convergence*. In the case where the coefficients are real and nonnegative, there is the following extension property: if the series converges on $\operatorname{Re} z > \rho$ as well as a neighborhood of ρ, then the series also converges on $\operatorname{Re} z > \rho - \epsilon$ [Prop VI.7].

Even more generally, the *Dirichlet ring* of arithmetic functions under Dirichlet convolution and pointwise addition neatly collects many of the relationships between various Dirichlet series. *Arithmetic functions* are functions $\mathbb{N} \to \mathbb{C}$, and the *Dirichlet convolution* is

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

In this ring we denote by ϵ the identity $\epsilon(n) = \delta_{1n}$, by 1 the constant function at 1, and by Id_k the kth power identity function defined by $\mathrm{Id}_k(n) = n^k$. Among many others, there are the relationships

$$1 * \mu = \epsilon, \quad \sigma_k = \mathrm{Id}_k * 1, \quad d = 1 * 1, \quad \phi * 1 = \mathrm{Id}, \quad \text{and} \quad \phi = \mathrm{Id} * \mu$$

with the usual notations for the Möbius, Euler totient, and divisor functions.

Dirichlet L series are variants of the zeta function that are associated to characters mod m, that is, a character of $G(m) = (\mathbb{Z}/m\mathbb{Z})^*$. Recall that the characters $\widehat{G}$ of a finite abelian group G are the homomorphisms $\chi \colon G \to \mathbb{C}^*$, that they satisfy the orthogonality relation [Prop V.4]

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{if } \chi = 1 \\ 0 & \text{else,} \end{cases}$$

and that there is a natural isomorphism into the double dual via evaluation [Prop V.3]. With χ a character mod m, its L function is defined by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \dfrac{\chi(p)}{p^s}}.$$

Note here we have another Euler product formula, and we will see that the zeta function associated to the mth roots of unity also has a corresponding Euler product. When $\chi = 1$ its L function differs from zeta only by $\prod_{p|m}(1-p^{-s})^{-1}$ hence still has a simple pole at $s = 1$, and when $\chi \neq 1$ it has abscissa of convergence 0.

The key property of L functions that Dirichet's theorem relies on is that $L(1,\chi) \neq 0$ whenever $\chi \neq 1$. To prove this, consider the zeta function associated with the field of mth roots of unity

$$\zeta_m(s) = \prod_{\chi \in \widehat{G(m)}} L(s,\chi) = \prod_{p \nmid m} \frac{1}{\left(1 - \dfrac{1}{p^{\mathcal{O}(p)s}}\right)^{\frac{\phi(m)}{\mathcal{O}(p)}}}$$

[Prop VI.13], where $\mathcal{O}(p)$ is the order of $p \in G(m)$. It is a Dirichlet series with positive integral coefficients. Furthermore, the only pole it can have is the simple pole at $s = 1$ coming from $L(s,1)$, so if $L(1,\chi) = 0$ for some $\chi \neq 1$, then ζ_m would be holomorphic at $s = 1$ hence holomorphic on $\operatorname{Re} z > 0$ by the extension property for Dirichlet series with nonnegative coefficients. But bounding the pth multiplicand in the Euler product via

$$\frac{1}{\left(1 - \dfrac{1}{p^{\mathcal{O}(p)s}}\right)^{\frac{\phi(m)}{\mathcal{O}(p)}}} = \left(\sum_{n=0}^{\infty} p^{-n\mathcal{O}(p)s}\right)^{\frac{\phi(m)}{\mathcal{O}(p)}} > \sum_{n=0}^{\infty} p^{-n\phi(m)s} = \frac{1}{1 - \dfrac{1}{p^{\phi(m)s}}},$$

it follows that

$$\zeta_m(s) > \prod_{p \nmid m} \frac{1}{1 - \dfrac{1}{p^{\phi(m)s}}} = L(\phi(m)s, 1),$$

which is impossible because then ζ_m has a pole at $s = 1/\phi(m)$.

Now the proof of Dirichlet's theorem is a matter of making esimates. Write

$$\sum_{p \in P_a} \frac{1}{p^s} = \frac{1}{\phi(m)} \sum_{\chi} \chi(a)^{-1} f_\chi(s), \quad \text{where we set } f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s},$$

[Lemma VI.9] using the orthogonality relation. For $\chi = 1$ observe $f_\chi \sim \log \frac{1}{s-1}$ as $s \to 1$ because f_χ differs from $\log \zeta$ by only a finite number of terms. On the other hand, for $\chi \neq 1$ the function f_χ remains bounded as $s \to 1$ since

$$\log L(s,\chi) = f_\chi(s) + \sum_{p,n \geq 2} \frac{\chi(p)^n}{np^{ns}},$$

where the left-hand side is bounded by the key property $L(1,\chi) \neq 0$ and the sum on the right-hand side is easily bounded [Cor 2 to Prop VI.10]. Hence the density of P_a is $1/\phi(m)$:

$$\sum_{p \in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(m)} \log \frac{1}{s-1}.$$

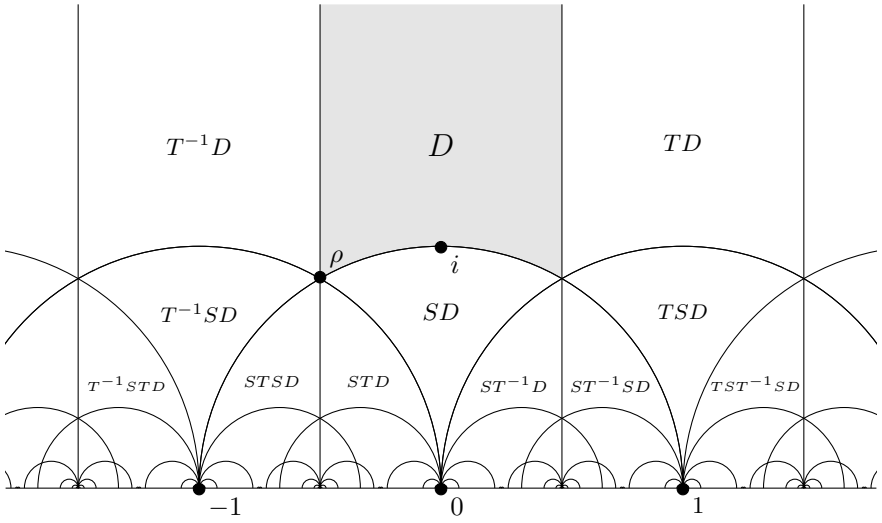
7. Modular forms

Modular forms are holomorphic functions on the upper half plane and infinity that satisfy a certain functional equation with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$. They are fundamental in number theory and appear in other areas such as algebraic topology, string theory, and also sphere packing, for instance via the packings determined by unimodular integral lattices.

The standard definition of a modular function is as follows. A *modular function of weight* $2k$ is a function on the upper half plane $\mathbb{H}$ that is meromorphic everywhere (that is, including infinity) and satisfies the functional equation

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

A *modular form* is a modular function that is holomorphic everywhere. Visually $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ via



where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and where D is the *fundamental domain* for the action of $\mathrm{SL}_2(\mathbb{Z})$. As suggested by the visual, the canonical map $D \to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ is surjective, and the restriction to the interior of D is injective [Cor to Thm VII.1]. Moreover

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \mid S^2 = (ST)^3 = 1 \rangle$$

[Thm VII.2 and remark], so when checking the functional equation it suffices to check it for S and T [Prop VII.1]. The condition for T implies f is determined in particular on a vertical strip of width one via $q(z) = e^{2\pi i z}$, so we set $f(\infty) = f(q(0))$.

The *Eisenstein series* G_k *of weight* $2k$ and *the weight 12 cusp form* Δ are basic examples of modular forms that are of fundamental theoretical importance. The Eisenstein series of index k for $k \geq 2$ is defined by

$$G_k(z) = \sum_{m,n}{}' \frac{1}{(mz+n)^{2k}},$$

where the sum runs over integers and the prime denotes avoiding $(0,0)$. It converges normally hence uniformly in D [Prop VII.4], so

$$G_k(\infty) = \lim_{z\to i\infty} {\sum_{m,n}}' \frac{1}{(mz+n)^{2k}} = {\sum_{n}}' \frac{1}{n^{2k}} = 2\zeta(2k).$$

The *weight 12 cusp form* arises from the bijection between $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ and isomorphism classes of elliptic curves [Sect VII.2.3]. In fact we have a bijection

$$\{\text{lattices on } \mathbb{C}\}/\mathbb{C}^* \cong \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$$

[Prop VII.3] induced by the map $(\omega_1,\omega_2)\mapsto \omega_1/\omega_2$, where this gives another way to define modular forms is as functions of the lattices of $\mathbb{C}$ up to homothety satisfying the analogous conditions $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ and $F(\lambda\omega_1,\lambda\omega_2) = \lambda^{-2k}F(\omega_1,\omega_2)$. For the claimed bijection, for a lattice Γ write its *Weierstrass function*

$$\wp_\Gamma(z) = \frac{1}{z^2} + {\sum_{\gamma\in\Gamma}}' \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}\right)$$

which has Laurent expansion

$$\frac{1}{z^2} + \sum_{k=2}^{\infty} (2k-1)G_k(\Gamma)z^{2k-2} = \frac{1}{z^2} + g_2 z^2 + g_3 z^4 + \mathcal{O}(z^6),$$

where $g_2 = 60G_2(\Gamma)$ and $g_3 = 140G_3(\Gamma)$ are constant. Morally, there should be a differential equation that $\wp$ satisfies because doubly periodic entire functions are constant, and indeed there is the relation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

This defines an elliptic curve. In fact the curve is isomorphic to the torus $\mathbb{C}/\Gamma$ both as groups and as Riemann surfaces, so as a bonus $\Delta \neq 0$ since the elliptic curve in the projective plane is nonsingular. Conversely, any elliptic curve has a doubly periodic Weierstrass function which determines a lattice. Therefore there is a bijection of lattices of $\mathbb{C}$ up to homothety and elliptic curves up to isomorphism, so it is valid to define one in terms of the other. As for the weight 12 cusp form, set $\Delta = g_2^3 - 27g_3^2$ to be the discriminant of the polynomial on the right-hand side. Given the values

$$\zeta(2) = \frac{\pi^2}{2\cdot 3}, \quad \zeta(4) = \frac{\pi^4}{2\cdot 3^2\cdot 5}, \quad \text{and} \quad \zeta(6) = \frac{\pi^6}{3^3\cdot 5}$$

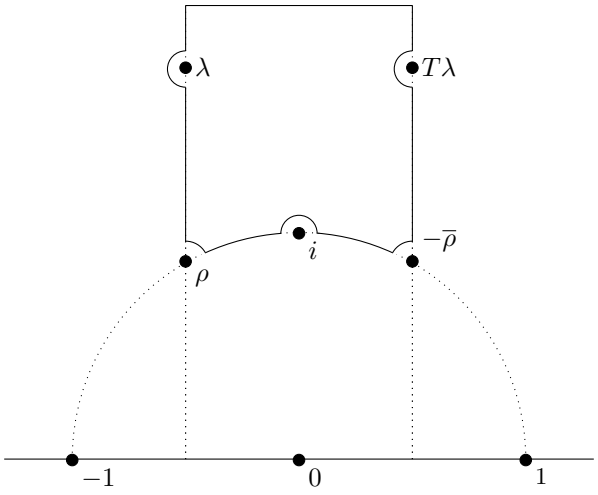
at once $\Delta(\infty) = 0$, and in general we call such a form a *cusp form*.

There is the surprising *valence formula*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + {\sum_{p\in\mathbb{H}/G}}^* v_p(f) = \frac{k}{6}$$

[Thm VII.3], which holds for a nonzero modular function of weight $2k$. Here $v_p(f)$ is the *order of f at p*, the integer n such that $f/(z-p)^n$ is holomorphic and nonzero at p, the $*$ denotes avoiding the classes of ρ and i, and the sum is finite because by isolation of poles and zeros of the meromorphic function f there is a neighborhood in D of ∞ containing neither hence a compact set in D containing all. To derive

the valence formula, integrate the following path counterclockwise



and use the argument principle:

$$\frac{1}{2\pi i}\oint_{\partial\Omega}\frac{f'}{f}\,dz = (\#\text{zeros} - \#\text{poles}) = \sum_{p\in\Omega}{}^{*} v_p(f).$$

To include a pole λ on one of the vertical lines, adjust the path symmetrically as shown to avoid its translate. As the radii of the circles approach zero, the value of the scaled integral around both ρ and $-\overline{\rho}$ is $-\frac{1}{6}v_\rho(f)$ and the value around i is $-\frac{1}{2}v_i(f)$ by considering the angle of the circle integrated. Moreover, the transformation S takes the left-hand arc on the unit circle onto the right-hand one and flips orientation, so since f satisfies

$$f(Sz) = f(-1/z) = z^{2k}f(z) \quad \text{and hence} \quad \frac{df(Sz)}{f(Sz)} = 2k\frac{dz}{z} + \frac{df(z)}{f(z)},$$

the contribution from both is just the integral of $-2k\frac{dz}{z}$ over one of the arcs, which is $k/6$. Now T takes the left-hand vertical segment onto the right-hand one while preserving orientation, so they cancel out. Finally $q(z) = e^{2\pi iz}$ takes the upper segment to a circle with negative orientation enclosing only a zero or pole of $f \circ q$, so it contributes $-v_\infty(f)$. Plugging everything in gives the desired formula.

The spaces of modular forms are formed by the Eisenstein series G_k and the weight 12 cusp form Δ. More precisely, denoting by M_k the $\mathbb{C}$-vector space of modular forms of weight $2k$, we have the following bases:

n	M_n	M_{n+1}	M_{n+2}	M_{n+3}	M_{n+4}	M_{n+5}
0	1	0	G_2	G_3	G_4	G_5
6	$\Delta M_0, G_6$	$\Delta M_1, G_7$	$\Delta M_2, G_8$	$\Delta M_3, G_9$	$\Delta M_4, G_{10}$	$\Delta M_5, G_{11}$
12	$\Delta M_6, G_{12}$	$\Delta M_7, G_{13}$	$\Delta M_8, G_{14}$	$\Delta M_9, G_{15}$	$\Delta M_{10}, G_{16}$	$\Delta M_5, G_{11}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮

[Thm VII.4], where this obviously shows the spaces are finite dimensional. The deduction of the table from the valence formula is straightforward. We have seen that the Eisenstein series G_k for $k > 1$ are modular forms. For $k = 1$, there is no

way to solve $n + \frac{1}{2}n' + \frac{1}{3}n'' = \frac{2}{6}$ over nonnegative integers, so there are no nonzero modular forms of weight 2. Similarly one shows that G_2 can only have a simple pole at ρ and that the same happens for G_3 at i and $\Delta = g_2^3 - 27g_3^2$ at ∞, so dividing by Δ gives an injection into the lower dimensions. In other words, the graded algebra $M = \bigoplus M_k$ is isomorphic to the polynomial algebra $\mathbb{C}[G_2, G_3]$ [Cor VII.2 and remark].

These results provide the basis for explaining the following phenomena:

- Bernoulli numbers appearing in $\zeta(2k) = \dfrac{2^{2k-1}}{(2k)!} B_k \pi^{2k}$ for $k > 0$
- divisor function values in $G_k(z) = 2\zeta(2k) + 2\dfrac{(2i\pi)^{2k}}{(2k-1)!} \displaystyle\sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$
- if f is a cusp form of weight $2k$, then $a_n = \mathcal{O}(n^k)$
- $\Delta = (2\pi)^{12} q \displaystyle\prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$, with $\tau(n)$ defined as these numbers.

[respectively Prop VII.7, Prop VII.8, Thm VII.5, Thm VII.6].

Theta functions count the vectors with various norms in integral unimodular lattices. According to Wikipedia:

> They are important in many areas, including the theories of Abelian varieties and moduli spaces, and of quadratic forms. They have also been applied to soliton theory. When generalized to a Grassmann algebra, they also appear in quantum field theory.

Consider a real finite n dimensional vector space V with a unimodular even definite integral lattice Γ of its dual V' so that in particular $\Gamma \in S_n$. Denote

$$r_\Gamma(m) = \text{ the number of elements } x \in \Gamma \text{ such that } x.x = 2m,$$

where we recall that $r_{\Gamma_8}(1) = 240$. The *theta function* of Γ is defined as

$$\theta_\Gamma(z) = \sum_{m=0}^{\infty} r_\Gamma(m) q^m = \sum_{x \in \Gamma} q^{\frac{x.x}{2}} \quad \text{where} \quad q = e^{2\pi i z};$$

it is a modular form of weight $n/2$ [Thm VII.8]. Normalizing the Eisenstein series $E_k = G_k / 2\zeta(2k)$ to have $E_k(\infty) = 1$ and using the fact that $\theta_\Gamma(\infty) = 1$, by taking a difference there exists a cusp form f_Γ of weight $n/2$ satisfying

$$\theta_\Gamma = E_k + f_\Gamma$$

[Cor 2 to Thm VII.8]. Moreover, it can be shown by purely working in the category S and attaching a more involved invariant denoted σ that if $E \in S_n$ is definite and even, then its rank is a multiple of 8 [Cor 2 to Thm V.2], so in this case V must have dimension a multiple of 8. Certainly there are only as many theta functions as there are isomorphism classes of lattices. We recall that this set is denoted C_n, where we determined $C_8 = \{\Gamma_8\}$ and $C_{16} = \{\Gamma_8 \oplus \Gamma_8, \Gamma_{16}\}$ and found the Leech lattice Λ contained in C_{24}.

Using these facts, we can determine $r_\Gamma(m)$ for various lattices Γ. In particular for the case $n = 8$, recalling that every cusp form of weight $n/2 = 4$ is zero since

$M_2 = \langle G_2 \rangle$, we have

$$\theta_{\Gamma_8} = E_2 = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m \quad \text{hence} \quad r_{\Gamma_8}(m) = 240\sigma_3(m) \quad \text{for } m \geq 1,$$

which generalizes the result $r_{\Gamma_8}(1) = 240$. For $n = 16$ again $M_4 = \langle G_4 \rangle$, so

$$\theta_\Gamma = E_4 = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m \quad \text{hence} \quad r_{\Gamma_8 \oplus \Gamma_8}(m) = r_{\Gamma_{16}}(m) = 480\sigma_7(m)$$

Here either of the lattices in C_{16} apply, so even though the lattices are not isomorphic, they have the same theta function which means they represent each integer the same number of times. The first nontrivial case is $n = 24$, where M_6 has basis

$$E_6 = 1 + \frac{65520}{691} \sum_{m=1}^{\infty} \sigma_{11}(m) q^m \quad \text{and} \quad F = (2\pi)^{-12}\Delta = \sum_{m=1} \tau(m) q^m.$$

Hence for any lattice $\Gamma \in C_{24}$ we have

$$\theta_\Gamma = E_6 + c_\Gamma F \quad \text{for some } c_\Gamma \in \mathbb{Q}, \quad \text{so} \quad r_\Gamma(m) = \frac{65520}{691}\sigma_{11}(m) + c_\Gamma \tau(m).$$

To determine $r_\Gamma(m)$, it remains to find the value c_Γ. We can do this by plugging in $m = 1$ and taking for granted known results for $r_\Gamma(1)$, for instance

$$r_\Lambda(1) = 0, \quad r_{\Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8}(1) = 3 \cdot 240, \quad \text{and} \quad r_{\Gamma_{24}} = 2 \cdot 24 \cdot 23,$$

the first of which we have seen before. Hence

$$\begin{aligned} c_\Lambda &= -\frac{65520}{691} = -\frac{2^4 3^2 \cdot 5 \cdot 7 \cdot 13}{691}, \\ c_{\Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8} &= \frac{432000}{691} = \frac{2^7 \cdot 3^3 \cdot 5^3}{691}, \\ \text{and} \quad c_{\Gamma_{24}} &= \frac{697344}{691} = \frac{2^{10} \cdot 3 \cdot 227}{691}. \end{aligned}$$

These are discrete combinatorial questions that are being answered by results falling out of the analytic study of theta functions and modular forms.

Acknowledgments

This expository paper was written for a reading course at UCSB organized in the Spring quarter of 2019. I thank Yitang (Tom) Zhang for supervising the reading course and Garo Sarajian for mentoring.

References

[1] Serre, Jean-Pierre. 1985. *A Course in Arithmetic.* New York: Springer.